Security for Enterprise Resource Planning Systems

Technical Report UTDCS-33-07
Department of Computer Science
The University of Texas at Dallas
August 2007
Wei She and Bhavani Thuraisingham

Security for Enterprise Resource Planning Systems

Wei She and Bhavani Thuraisingham
wxs061000@utdallas.edu bhavani.thuraisingham@utdallas.edu
University of Texas at Dallas, Richardson, TX, USA

Abstract

Enterprise Resource Planning (ERP) is the technology which provides the unified business function to the organization by integrating the core processes. ERP is experiencing the transformation which will make it highly integrated, more intelligent, more collaborative, web-enabled and even wireless. ERP systems have to be secure. Many ERP vendors are integrating security into their products. While these security solutions may work for a closed environment, we need new approaches for an open environment. This paper introduces ERP technology from its evolution through architecture to its products. The security solutions as well as directions for secure ERP systems are also presented.

Keywords: Enterprise Resource Planning, Exchange Infrastructure, RBAC, Authorization, Security Policies, Web Services, SOA,

1. Introduction

Enterprise Resource Planning, an approach for the business integration, has been widely deployed in various kinds of organizations since it was defined by Gartner Group in the 1990s as the next generation of Manufacturing Business System and Manufacturing Resource Planning software. Today, ERP is considered to be "the price of entry for running a business" [1]. An ERP system is an integrated, configurable and tailorable information system which plans and manages all the resources and their use in the enterprise, streamlines and incorporates the business processes within and across the functional or technical boundaries in the organization. With ERP, an enterprise can automate its fundamental business applications, reduce the complexity and the cost of the collaboration, force the enterprise itself to take part in the Business Process Reengineering (BPR) to optimize its operations and finally result in the decreased operation costs and increased profits.

This objective of this paper is to give a comprehensive discussion of the state of the art in ERP technology and the security issues for an ERP system. In particular, we discuss the evolution of ERP, the key components of ERP, the status with vendor products and also what has been done with respect to security. Our research as well as plans for secure ERP systems will also be discussed.

The organization of this paper is as follows. The history and evolution of ERP systems will be given in section 2. ERP technologies and framework including the communication platform such as EDI, ALE and Exchange Infrastructure are presented in section 3. Section 3 also includes a discussion of the ERP architecture, some aspects of SAP and the emerging web services for ERP. Major ERP vendors and their products are discussed in section 4. Security issues for ERP systems are discussed in section 5. In particular, the overview of the ERP security using a layered approach, as well as the RBAC model for ERP is discussed. We will compare these security features with the authorization function in SAP R/3 system and the Baan security solution. Some trends for ERP systems as well as security are discussed in section 6. The paper is concluded in section 7.

2. History of ERP Systems and Applications

The history of ERP traces back to 1960s when most organizations were developing the centralized computing systems using Inventory Control Packages (IC) in order to automate their inventory control systems. These legacy systems are mostly based on the programming languages such as COBOL and FORTRAN. Material Requirements Planning (MRP) systems were developed in 1970s in order to provide the requirements planning of products, and Manufacturing Resources Planning (MRP II) in 1980s to provide the optimization of the manufacturing processes. ERP emerges in early 1990s as an enterprise-wide and across-functional integration of the core organizational business processes

including manufacturing, distribution, accounting, financial, human resource management, project management, inventory management, service and maintenance. From the point of view of some researchers, the ERP technology after 2000 is considered as "Extended ERP" [2] because e-business solutions such as Customer Relationship Management (CRM) and Supply Chain Management (SCM) are included into the core modules of original ERP systems.

In "Extended ERP" systems, the "add-ons" may include many of the modules which are more likely to be used in some specific business domains. By providing more and more of components, ERP extends its edge into many other areas. Today, ERP has been utilized into the following industrial and non-industrial areas: Aerospace and Defense, Banking, Consumer Products, Construction, Healthcare, Education and Research, Insurance, Raw and Processed Materials, Logistics, Transportation, Wholesale, Public Sector, and Telecommunications. Furthermore, ERP systems are being used extensively for applications such as accounting, human resources management, planning and scheduling. More recently e-business and outsourcing applications are also relying on ERP systems.

Various commercial products including from SAP, Oracle and Baan are not available in the marketplace. Furthermore, web services and service oriented architectures are the major underlying technologies for emerging ERP systems. Security including confidentiality, privacy, trust, integrity and data quality and pedigree features are important for ERP systems. The next three sections will discuss ERP technologies, products and security issues.

3. ERP TECHNOLOGY

3.1 Overview

ERP systems have evolved extensively over the years. Initially such systems were used for simple accounting and human resources applications. With the advent of the web technologies, companies such as Oracle, SAP and Baan are developing a suite of applications for ERP systems. Furthermore, the emerging web services are having a major impact on ERP systems.

In this section we will discuss the various components of ERP systems. We will start with a discussion of the basic components in section 3.2 including Electronic Data Exchange (EDI), Application Linking and Embedding (ALE) and Intermediate Document (IDoc). Next we will discuss SAP's exchange infrastructure that is cornerstone to ERP systems in section 3.3. An overview of ERP architecture will be discussed in section 3.4. Finally emerging web services and their relationship to ERP systems will be discussed in section 3.4.

3.2 EDI, ALE and IDoc

Electronic Data Interchange (EDI), which is also called "paperless exchange" [3], is the technology that allows the enterprises to exchange business information between separate computer systems, using a standard structured format over a communication network. EDI technology, which has already been around for many years, is the footstone of all the ERP technologies. It brings lots of benefits to the modern business process including: less data errors, less processing time, less paperwork, lower cost, less inventories, less planning, standardization, and better business processes. The most important is that EDI technology enables the integration within and across the enterprises. What an EDI system needs to do is to "translate" the documents between the internal format and the standardized format so that the outbound e-documents can be recognized by the receiver and the inbound e-documents can be correctly transferred to the style which is able for the company to read. To fulfill the tasks of translation, a third-party translator will usually be integrated into the system, so EDI system can send and receive the e-documents via the network in the standard form which is called EDI message. To provide this standardization, a committee name ANSI X.12 was formed in 1975 and ANSI ASC X.12 was published in 1979. Now most of the companies are more willing to adopt another international standard, EDIFACT, which was published in 1980s.

Application Link Enabling (ALE) and Intermediate Document (IDoc) are SAP's proprietary technologies that help integrate the business processes within an organization; they are the basis of SAP's business framework architecture. The ALE technology contains an outbound process, an inbound process and an exception-handling process, and IDoc is the standard of the messages which flow between the functional components. Once an application document is created, an outbound process is immediately triggered and the ALE Service Layer will be requested to determine whether any other components may be interested in this information. At this time, the document will be read from the database and formatted into Master IDoc and sent to the ALE Service Layer. ALE Service Layer will generate the communication IDocs from the Master IDoc and deliver them

to the intended components. The inbound process sill store the communication IDoc into the database, and a posting program will be triggered to read the IDoc and the document will be created and delivered to the application program.

3.3 SAP Exchange Infrastructure

With EDI and ALE technologies, distributed business processes within an enterprise have the ability to communicate with each other via one-to-one links. In a small enterprise which has a small number of components, one-to-one communication is the best way to integrate the business processes as it can be achieved with ease. But in cases where a large number of components are involved, this will bring higher complexity and cost of communication and negative impact on the stability of the environment. In this situation, a common communication infrastructure that allows the central management of the information will avoid these complications and bring more flexibility for expanding the business.

SAP Exchange Infrastructure [4] is the layer of SAP NetWeaver – SAP's integration platform for integrating heterogeneous components in a system landscape. Furthermore, with SAP Exchange Infrastructure, it is possible to create the business processes across the distributed systems which may be SAP or non-SAP systems.

The integration using SAP Exchange Infrastructure is achieved by exchanging the messages in open standards such as Extensible Markup Language (XML), and the Simple Object Access Protocol (SOAP). In the design stage, the specific integration information will be stored into the Integration Directory and Integration Repository and in the run time, they can be used for the routing and mapping. The SAP Exchange Infrastructure has the following components:

- Integration Repository that stores integration knowledge from the design time.
- Integration Directory that stores the knowledge that describes the integration-related parts of the customer landscape.
- Integration Server which contains an Integration Engine and receives the exchanged messages, determines the receiver, performs the mapping and routes the messages to the receiver system.
- Integration Monitor which monitors the exchange infrastructure.

While the SAP exchange infrastructure is the cornerstone to the ERP architecture, there are many other components to the architecture. These components are discussed in the next section.

3.4 ERP Architecture

There are many disadvantages in the MRP II and MRP technologies. In an enterprise, some of the systems may be developed by the enterprise itself, while others may be developed by different vendors using different databases, languages and technologies. Systems are different from each other which makes it unable to upgrade the organization's businesses, strategy and information technologies in an effective way. With the communication infrastructure and the ERP functionalities encapsulated in components, an ERP system can easily meet these requirements. A typical ERP system should at least have the following features:

- Componentized: different business functionalities are designed as different components.
- Centralized: all the components share a centralized database management system.
- Integrated: components are integrated and seamless data flow between components allows them to collaborate as one function.
- Flexible: system is expandable and compatible with the old systems, the change to the business processes and strategies are easy to fulfill.
- Configurable & tailorable: system should be easily configured according to the enterprise's needs.
- Real-time: the components work in real time, online and batch processing modes should be available.

The business logic in ERP system employs client/server architecture to create a distributed computing environment. In the general case, the three-tier architecture will be used, which contains three layers of logic:

- Presentation Layer (Front): A unified Graphical User Interface (GUI) or browser which collects input, generates requests and returns the results back to the user.
- Application Layer (Middle): Application programs which collect the requests from the Presentation layer and process the requests based on the business rules, functions or logics.
- Database Layer (Back): RDBMS which manages the operational and business data throughout the whole enterprise and the user access to this information.

As the basis of the ERP system, an information exchange platform such as SAP NetWeaver will always be deployed

before implementing ERP software. After consolidating the business logic and the technical platform, we will have the ERP system architecture as shown in Figure 2.

The components that different ERP vendors provide may vary, yet the core functionalities are nearly the same. These functionalities include:

- Financial Management which may include the functions such as collection and payment management, payables and receivables management, assets and properties management, cash management, loans, financial consolidation, general ledger, treasury management, and planning & budgeting.
- Human Resource Management which may include the functions such as payroll management, self-service, learning management, benefits, recruitment, tutor, timer and labor management, and compensation management.
- Manufacturing Management, which may include functions such as discrete manufacturing, process manufacturing, flow manufacturing, manufacturing scheduling, and shop floor management.
- Sales, Distribution and Logistics Management which may include functions such as order capture, services, sales, sales incentive management, pricing, logistics, bulk stock management, inventory management, warehouse management, requirements management, and strategic account planning.

The following features may be grouped by some researchers and ERP vendors into the solutions within the scope of e-commerce, yet we can also include them as part of ERP system (note: M. A. Rashid considers them as extensions of ERP [2]).

These features are

- Customer Relationship Management
- Product Lifecycle Management
- Supply Chain Management
- Supplier Relationship Management (Procurement)
- Business Intelligence

The components of an ERP system can work as separate units which can be built into other ERP systems, or they can be combined as an entire suite to implement. The enterprises can choose the most appropriate solution, purchase the components from different vendors and put them together.

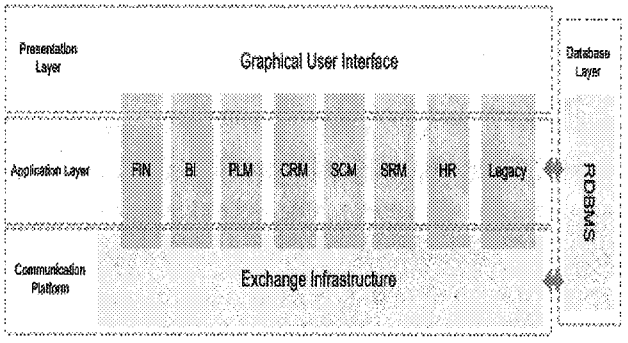

Fig. 1 The architecture of enterprise resource planning

3.5 Web Services

It is stated in [9] that we are now in the third wave of ERP systems. The first wave was related to manufacturing applications. The next wave was specialized applications such as supply chain management. The third wave is based on web services.

The use of web services eases integration and also reduces cost. Clients want to access information without having to go thorough all the ERP software. Therefore with the use of web services and the composition of web services, clients as well as out sourcing vendors can access many of the ERP applications seamlessly. These applications include checking bank accounts, placing orders and other services. Reduction in cost comes from the fact that through web services, clients can communicate with legacy ERP software and do not have to deal with the complexities of the software. Also the ERP vendors are introducing Web Scenarios broker Hub that will act as a broker between the web services and the ERP software. SAP offers this hub through mySAP and Oracle offers it via its E-business suite.

Note that the infrastructure for the web services is Service oriented Architectures (SOA). That is, web services are hosted on SOAs. SOAs provide the support to integrate and compose web services. In the emerging ERP systems, the various functions are implemented as web services and the infrastructure is based on SOAS.

4. Vendors and Products

In this section we will provide an overview of the major vendors of ERP systems. SAP is one of the prominent vendors of ERP. Other vendors include Peopesoft and Baan. However Peoplesoft has been purchased by Oracle and Oracle is emerging has a major vendor of ERP systems. Furthermore,

Oracle provides the server technologies that the ERP applications could utilize while SAP and Baan rely on various vendor products for server technologies. Note that Baan is now purchased by SSA. Microsoft is also becoming a player in ERP software. We will discuss the essential points in various products.

SAP (Systems, Applications and Products in Data Processing) was formed in 1972 by five former IBM employees in Germany. It focuses on the development of application software for real-time business processing with its first accounting software developed in 1973. Its first ERP product, SAP R/2, was developed in late 1970s using a centralized database and dialog control system. In 1990s, SAP R/3 which uses the three-tier architecture of database, application and user interface was unleashed on the market. R/3 was a breakthrough which made SAP become the largest vendor in the ERP market by 1999. By 2005, there were around 100,000 installations around the world, more than 1,500 partners, over 25 industry-specific business solutions, and more than 30,000 customers in over 100 countries. SAP now owns 26% of CRM market share, 29% of ERP market share and 19% of SCM market share by total software revenue. SAP NetWeaver unifies the integration technologies into a single platform which lays the foundation to integrate all the systems which runs SAP or non-SAP software. It is the basis of SAP ERP applications, partner solutions and custom-built applications. SAP R/3 is the third generation set of highly integrated software which performs the core business functions within a company; while mySAP which also includes R/3 component as an important building block will be more intended to empower the collaboration between organizations. mySAP is a web-based e-business suite.

Oracle, which was founded in 1970s in USA, is most famous for its well-known relational database Oracle and is the second largest software company in the world. In 1987, Oracle offered its first ERP software – Oracle General Ledger. In the following years, Oracle developed other ERP software such as self-service applications, strategic procurement solution, financial consolidation engine, and flow manufacturing product. Oracle's ERP system is known as Oracle E-business Suite which has more than 50 different modules covering the following areas: finance, accounting, human resources, manufacturing, supply chain management, project and front office. Oracle also has many other well-reputed products in other fields such as database, data warehousing, and workflow. After the acquisition of PeopleSoft and JD Edwards in 2004, Oracle gains approximately 22% of the ERP market share. PeopleSoft Enterprise is the business application suite that offers web services integration with multi-vendor and homegrown applications; it is admittedly considered as easier to configure and more flexible than its competitors.

JD Edwards: JD Edwards EnterpriseOne and JD Edwards World are both the business applications from J.D. Edwards Company that has a vast experience in supplying software for the IBM iSeries platform. JD Edwards World provides the web-enabled applications for the management of plants, inventories, equipments, finances and people.

Sage, which was founded in England in 1981, entered the ERP market and gained a solid market share using the strategy of acquiring small ERP vendors such as Tetra, Interact Commerce Inc. By 2005, Sage has revenues of $1.4 billion in ERP market and claims 6% of the market share as the third largest ERP vendor. Sage Line 500 v6 is the newest version of the Sage Line 500 product family which is the web-based integrated ERP solution covering core functionalities in a company. Sage 1000 is new, single business management software which is designed to offer the operations within mid-size organizations.

Microsoft, founded in 1975, is the biggest software company in the world with its famous Windows series products. Microsoft Business Solution Group (MBS) is the department which focuses on providing the ERP solutions, such as Microsoft Dynamics (formerly Microsoft Business Solutions) which is the integrated business management solution which includes financials, customer relationship management and supply chain management. By 2004, MBS has the revenue of around $800 million which gives it a 4% of ERP market share.

Others: In addition to the above vendors there are several other ERP vendors. In 2004, the biggest ERP vendors – SAP, Oracle, Sage, Microsoft and SSA accounted for around 70% of the ERP market share by the revenues. The other 30% is shared by other ERP vendors such as Geac, Intentia, Infor Global Solutions and Lawson.

5. Security in ERP

5.1 Overview

Security is critical for ERP systems as they are being applied to numerous industries including defense, intelligence, medical and financial. First of all we need to develop a security policy

and a model for ERP systems. Many of the current systems focus on confidentiality aspects of security. In this section we will discuss the developments as well as trends in security for ERP systems.

In section 5.2, we discuss what needs to be secured. Policies are discussed in section 5.3. Then in section 5.4 we will discuss current developments including security for SAP. In section 5.5 we will discuss some of the next generation security models. In section 5.6 we will provide an overview web services security as the emerging ERP systems are based on service oriented architectures. .

5.2 Approaches to Security

The security problems exist in every facets of an ERP system. These facets can be classified into three categories which are network layer, presentation layer and application layer which includes business processes, internal interfaces and database.

When a customer/partner communicates with an ERP system, or the business components located in different sites communicate with each other, the security issues are grouped into the network security domain. ERP security research is not involved with network security. It is expected that the various network security products will ensure communication security.

The presentation layer refers to the graphical user interface (GUI), browsers and PCs. Since the transmission of GUI packets is impossible to restrict, ERP security at the UI level is achieved by limiting the user access to GUI. One way to provide security to a certain extent may be just inserting a CITRIX server between the user and the ERP system.

The security in the application layer is the main focus of the ERP researchers to secure the business data and processes. The technicians will also choose to activate/deactivate the security functions provided by the database vendor according to the overall security solution. ERP research also focuses on the infrastructure security aspects such as secure web services tailored for ERP applications. Reind van de Riet has summarized in his paper (see [5]) some of the security aspects in ERP system:

- Security Policy and Administrator: ERP researchers have to specify explicit and well defined security policies that can be easily defined and maintained. The security policies will offer the rules for the access of subject to object, and these are the constraints put on the administrators when they are granting/denying permissions to the users.
- User Authentication: to verify whether the user is the same person as he claims.
- Separation of Duties: tasks must be classified such that certain tasks can only be performed by certain users or roles.
- Authorization: to verify whether the user has the access to the relevant resources. Depending on the authorization rules, user is granted access.
- Time Restriction: the access is permissible only during certain time.
- Log and Trace: the logging and tracing of relevant events has to be done with preventing the log files from breach.
- Database Security

Essentially we need end-to-end security for ERP systems. The next three subsections discuss some of the current trends and directions for secure ERP.

5.3 Policies

Much of the focus on ERP security has been on confidentiality. Confidentiality is about granting access to users depending on their access permissions. However we need to include other types of policies. These include the following:

Need to know policies: These are policies where access is granted based on whether a user needs to know. These policies are enforced in military environments.

Need to share policies: There is now a migration from need to know to need to share policies where organizations including military, financial, and healthcare agencies have to share data to carry out their operations. We discuss need to share policies in our paper on Assured Information Sharing [9].

Trust policies: These policies ensure that data is shared only between individual organizations that are trusted.

Integrity policies: These policies ensure that data is modified by authorized individuals. Furthermore, data provenance and data quality policies that determine where the data has traveled and the accuracy of the data may also be included under the integrity policies.

5.4 Current Solutions

5.4.1 Role-Based Access Control

Many of the current systems are based on Role-Based Access Control (RBAC). This model (Figure 3) defines roles and grants certain access rights. According to [6], an RBAC model consists of the following components:

- Permissions: Permission is the access to one or more objects in the system. The permission has different meanings in different environment. In a database system, the permission refers to the rights such as select, update, delete or insert a record. In an accounting application, it may be the rights such as account creation/deletion, credit/debit and transfer. [6]
- Roles: A role is a named job function within the organization. A role may be hierarchical. For example, an engineer role is also an employee role.
- Users: A user is a human being who may be assigned to one or more roles.
- Constraints: In the system where there is only one single administrator, the constraints may be meaningless. If the administration is decentralized, which means there are several administrators, the constraints will be used by the senior administrator to restrict the junior administrator's right to grant/deny the permissions.

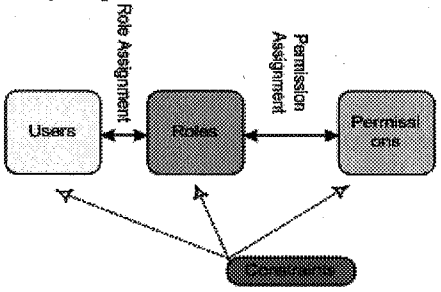

Fig.2 The model of role-based access control

5.4.2 Authorization in SAP R/3

Some of the concepts involved in the authorization in SAP R/3 system are listed below [7]:

- Authorization Object, which represents the authorization concept and consists of some authorization fields.
- Authorization, which is an instance of one authorization object and defines the permitted value range of each authorization field of the authorization object.
- Authorization Profile, which contains some authorizations which are assigned to the user by the administrator.
- Authorization Check, which is used to protect the transactions or data you choose, and is embedded in the program logic. When the authorization check is performed, the authorization profile will be used to compare with the required values to run the specific transaction.
- User Master Record, which enables the users to log into the R/3 system and grant limited access to the transactions and data.
- Profile Generator, is the component that helps the administrators create, generate and assign authorization profiles using activity groups and user.

A profile generator may have the following components:

- Activity Group is a collection of activities such as tasks, reports and transactions. An activity group usually represents a job in the enterprise. An activity group can have many users assigned to it, and a user can also be assigned to many activity groups. An activity group can be assigned to the following types of users: user ID, job and position. Job represents the general classification of duties. Position represents a person's detailed individual assignment within an enterprise. The difference between job and position is that job is just the title which does not imply what projects you will do in the company, while position does so.
- Composite Activity Group is the collection of several activity groups.
- User Assignment is the task that assigns one or more users/roles/positions to one or more activity groups or composite activity groups.

Another important concept in the authorization in R/3 is Authorization Administration which means whether the creation, generation or assignment of authorization is centralized or decentralized (one or more administrators).

Through these concepts, we may learn that the mechanism of R/3 authorization is actually an instance of Role-Based Access Control Model, except that it contains some elements specifically used in R/3 environment. Figure 4 provides a visual understanding of the model of authorization in R/3 system. Furthermore, Logging and Tracing is also a required component to secure the application layer of ERP system, although it is not the key function.

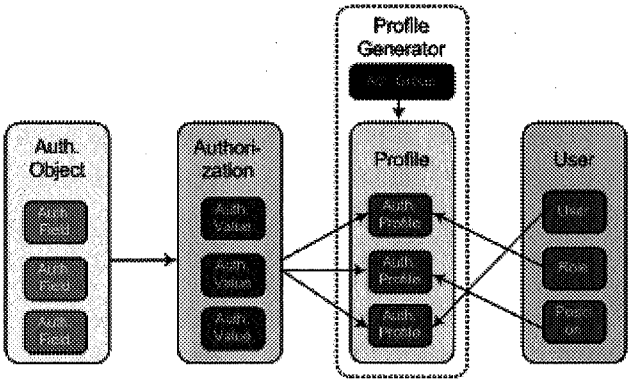

Fig. 3 The model of authorization in r/3

5.4.3 Baan Security using DEM

In Baan (now purchased by SSA) security architecture, the solution is based on the RBAC model. Baan security solution is using a tool named Dynamic Enterprise Modeler (DEM) to assist the security configuration of Baan. DEM is used to model business processes or functions of an organization and defines the roles. Within the architecture of Baan's security solution, there are four concepts: User, Employee, Role and Process.

- User: Baan user is a profile including all the personal information of an employee.
- Employee: The human being who works in the organization.
- Role: Role is defined to indicate the position and the assignments of the employee. All employees must be assigned to a role, and roles will be assigned to the business processes.
- Process: Once a process is modeled in Baan ERP, roles will be attached to that process.

5.5 Next Generation Models

5.5.1 Extended RBAC

Most of the contemporary ERP software adopts traditional access control methods such as RBAC as its primary measure to secure the system. What these methods care is whether some subject is allowed to perform the requested rights on the object. In some cases, the subject has to meet some mandatory requirements before exercising the rights. A good example is that the researcher has to fill in his/her personal information before he can have the rights to read or download the white papers. This mandatory requirement is Obligation [8]. Another important requirement for accessing the resources is the environmental or system requirement which is called Condition [8] such as accessing time, date and location. Since these functional predicates are not included into the idea of traditional access control methods, a straightforward enhancement of RBAC is to introduce obligation and condition predicates.

In this ERBAC model, an extra decision manager is added since obligation and condition predicates will be taken into account. In the decision process, condition requirements will be checked first; if all the environmental conditions are met, the checking procedure for the obligations will be triggered; and the decision process will check whether the user is intended to access the information. Srinivasan and Thuraisingham are examining the extended RBAC model for ERP [15].

5.5.2 UCON

In recent years, a new model called the Usage Control Model (UCON) was proposed in order to set up a framework for the future security techniques in ERP. UCON not only integrates three functional predicates: authorization, obligation and condition, but also brings in the concept of time. This feature allows a security component in ERP system to be far more dynamic than before [8].

UCON model consists of the following core components:

- Subject and subject attributes: An entity with associated attributes which holds or exercises certain rights on objects.
- Object and object attributes: An entity with associated attributes that one or more subjects hold or exercise rights on.
- Rights: Privileges that a subject can or cannot access an object.
- Authorization: Functional predicate determining whether a subject is allowed to perform some right on an object.
- Obligation: Functional predicate verifying whether the mandatory requirements have been fulfilled before a subject performs some right on an object.
- Condition: Functional predicate that checks whether the current environmental or system status allows a subject to perform some right on an object.

UCON model is a large model family in which one can have different combinations of the above three predicates. If we regard the UCON model with only one of these predicates used as the leaf node, we can build up a tree rooted at $UCON_{ABC}$ model. These models are denoted $UCON_A$, $UCON_B$, and $UCON_C$. These models will be divided into several sub models based on whether time is taken into consideration. For example, $UCON_A$ will be divided into $UCON_{preA}$ and $UCON_{onA}$. Furthermore, these sub models can be divided into more detailed models depending on when and whether the update of mutable attributes will occur. We are currently investigating the applicability of UCON features for ERP security.

5.6 Web Services Security

As we have mentioned earlier, web services and service oriented architectures (SOA) are key technology for emerging ERP systems. Vendors such as SAP and Oracle are migrating their products based on three-tier architectures to web-based SOAs. Therefore, securing web services and service oriented architectures are critical for securing emerging ERP systems.

Various efforts have been reported on securing web services [10]. Furthermore, standards such as OASIS have developed security specifications including SAML (Security Assertion Markup Language) and XACML (XML Access Control Markup Language) [11]. In addition securing XML documents as well as securing semantic web technologies has received attention [12], [13]. Programs such as the Department of Defense Global Information Gird (GIG) have focused on security for service oriented architectures [14]. However little work has been reported on adapting the various technologies for securing ERP. This will be the major challenge.

6. Trends

Looking back at the history of ERP technology, we can find that the transformation from mainframe structure into the client/server architecture has been a major step. With this architecture, it became possible to develop a large system which integrates lots of functionalities. Today, ERP has become the core of the operation and business in a company. With the emergence of the web, ERP systems will be web-based. We can expect the future of ERP system to include the following features:

- Heterogeneity: Heterogeneous/heterogeneity means that the components from different vendors coexist and cooperate in an ERP system. It has two prerequisites: componentization and integration. It is true that some of the leading ERP vendors are going to or have already done something in these two aspects. Stronger communication platforms are provided to support heterogeneous applications and applications are developed in the form of components.
- Collaborative: This could be in the realm of e-business. We can classify the business processes within an enterprise into two types: enterprise-centric process and collaborative process. Processes such as accounting and payroll processing are enterprise-centric; while others such as supply chain management are almost completely collaborative. There are some intervenient processes, yet they are designed and developed in an enterprise-centric way. In the future, more of the processes will be redesigned in a collaborative way. This feature also implies that the ERP system will be more open and web-based.
- Intelligent: ERP system will include more components which carry out analysis, investigation or even advice on strategic transformation. This feature implies that more confidential information will flow within or out of an ERP system.
- Web-based: With the emergence of the web, it is natural that the functionalities or services will become web-based, which will make the system highly vulnerable to the security threats.
- SOAs and Web Services: As we have stressed in this paper, future ERP systems will be based on SOAs. Such architectures provide the infrastructure to integrate and compose multiple web services.
- Wireless: Access to the ERP system from a mobile device.

Currently, to secure an ERP system, there are two methods: access control and logging. However there are factors that may prevent corporations from incorporating security into their ERP system. One reason is due to the cost and time. Furthermore, stringent security controls make the operation more complex and difficult to use. In a large enterprise, there will be many activities that may change an employee's authorization level, such as promotion or reassignment. This will make the user-based access control difficult to implement. Logging systems that involve the logging of detailed activities are costly and may have low performance as they have to trace every event and log all activities. As ERP systems become web-based, the security issues within an open system become critical.

Usually, the better security solutions will results in higher cost and lower performance. This contradiction exists in any system. However, ERP subsystems are used to lower the cost and increase the profit of an enterprise; hence the performance of the system will be considered as most important by the executives of an enterprise. While there are important factors that may deter security, security is crucial to protect the data and the processes. Therefore we need flexible security policy management and enforcement. There are times when security has to be overlooked to achieve performance, especially for real-0time applications. However, in such situations, the implications of violating security have to be studied at length and appropriate actions have to be taken.

7. Conclusion

This paper has provided an overview of ERP system as well as security for ERP systems. ERP is the technology which drives the reformation in the realm of economy and impacts people's life styles indirectly. In the ensuing years, we expect ERP systems and applications to be more integrated and intelligent. Furthermore, such systems will be web-based, service oriented and even wireless. The security issues for ERP systems have been present for a while, but due to the closed environment with current ERP systems, not much research has been carried out in

security. However, with the open environments of the future, ERP security must be emphasized and much research has to be carried out. In particular, we need end-to-end security for an EEP system. The research should focus on several aspects including the following:

- Securing the transferred data
- Developing user authorization methods
- Enhancing the logging mechanism
- Securing the database
- Securing the operating system
- Securing web services

We also need to examine the interfaces between the different components (e.g. operating system, database systems, Logging component etc.) and ensure that the interfaces are secure. Essentially research should focus on a policy, model and design of a secure ERP system. In addition, web services security and secure service oriented architectures are emerging as a major technology for secure ERP systems.

Our research is proceeding in two directions. One is securing applications such as supply chain management which is an integral part of ERP system. The other is securing the infrastructures such as secure SOAs and web services. The various functions of an ERP will be executed as web services. These web services are integrated using SOAs. Therefore, by examining security for supply chain management as well as SOAs we are providing a comprehensive solution for securing ERP systems.

References

[1] K. Kumar, and J. van Hillegersberg. "ERP Experiences and Evolution". Communications of the ACM. Vol. 43. No. 4. Apr. 2000.

[2] M. Rashid, L. Hossain, and J.D. Patrick. "The Evolution of ERP Systems: A Historical Perspective". In Idea Group Publishing, 2002.

[3] A. Nagpal, G. M. de Bruyn, and R. Lyfareff. "ALE, EDI & IDoc Technologies for SAP". pp. 6-20, 376-384. Prima Publishing. 1999.

[4] White Paper, "SAP Exchange Infrastructure 2.0", SAP AG and Sun Microsystems. 2002.

[5] R. van de Riet, W. Janssen and P. de Gruijter. "Security Moving from Database Systems to ERP Systems". Database and Expert Systems Applications, 1998. Proceedings. pp. 273-280. Aug. 1998.

[6] Ravi S. Sandhu, Edward J. Coyne, Hal L. Feinstein, and Charles E. Youman. "Role-Based Access Control Models". IEEE Comput. Vol. 29. No. 2. Feb.1996.

[7] White Paper. "Authorizations Made Easy *User Role Templates and Generating Authorization Profiles*". Release 4.6A/B. SAP AG. 2000.

[8] J. Park and R. Sandhu. "The $UCON_{ABC}$ Usage Control Model", ACM Transactions on Information and System Security, Vol. 7, No. 1, February 2004.

[9] B. Thuraisingham. "Assured Information Sharing". UTD Technical Report, 2006.

[10] E. Bertino et al. "Security for Web Services". Proceedings IEEE Web Services Conferences, 2004.

[11] OASIS. "Security Specifications". http://www.oasis-open.org/specs/index.php.

[12] E. Bertino et al. "Authentic Publication of XML documents". IEEE Transactions on Knowledge and Data Engineering, 2004.

[13] B. Thuraisingham. "Security Standards for the Semantic Web". Computer Standards and Interfaces Journal, 2005.

[14] GIG/IA. "National Security Agency Presentation". 2005. http://www.nsa.gov/ia/industry/gigir.cfm?MenuID=10.3.2.2.

[15] I. Srinivasan and B. Thuraisingham. "Extended RBAC for ERP Systems". Technical Report, the University of Texas at Dallas, November 2006.

[16] B. Thuraisingham. "Database and Applications Security *Integrating Information Security and Data Management*". pp. 2-19. Auerbach Publications. 2005.

[17] White Paper, "SAP R/3 Enterprise (version 1.0)". SAP AG. 2002.

[18] White Paper, "SAP Exchange Infrastructure 2.0 *Technical Infrastructure*". SAP AG. 2002.

[19] A. H. Bakry, and S. H. Bakry. "Enterprise resource planning - a review and a STOPE view". International Journal of Network Management. 15. pp. 363-370. 2005.

[20] E. M. Shehab, M. W. Sharp, L. Supramaniam and T. A. Spedding. "Enterprise resource planning - an integrative review". Business Process Management Journal. Vol. 10. No. 4. pp. 359-386. 2004.

[21] R. L. Glass. "Enterprise Resource Planning - Breakthrough or Term Problem". The Database for Advances in Information Systems. Vol. 29. No. 2. Spring 1998.

[22] D. Sprott. "Componentizing the Enterprise Application Packages". Communications of the ACM. Vol.43. No.4. Apr. 2000.

[23] L. Iacovou, I. Benbasat, and A. S. Dexter. "Electronic Data Interchange and Small Organizations : Adoption and Impact of Technology". MIS Quarterly. Vol. 19. No. 4. pp. 465-485. Dec. 1995.

[24] P. Jayaweera, P. Johannesson, and P. Wohed. "Collaborative Process Patterns for e-Business". Siggroup Bulletin. Vol. 22. No. 2. Aug. 2001.

[25] A. Kern, M. Kuhlmann, A. Schaad, and J. Moffett. "Observations on the Role Life-Cycle in the Context of Enterprise Security Management". SACMAT'02. June 3-4. 2002.

[26] E. Goodman. "Security Evaluation and Management for the SAP R/3 Environment". GSEC Certification Practical. 2004.

[27] A. Schaad. "Panel: Security in Enterprise Resource Planning Systems and Service-Oriented Architectures". SACMAT06. 7th Jun. – 9th Jun. 2006.

[28] G. Valente. "Baan Application Security". Deloitte Touche Tohmatsu. 1998.

[29] S. Megaache, T. Karran, G. R. Ribeiro Justo. "A Role-based Security Architecture for Business Intelligence". Technology of Object-Oriented Languages and Systems, 2000. TOOLS 34. Proceedings. 34th International Conference on. pp. 295 - 305. 30th Jul. - 4 Aug. 2000.

[30] W. Brown. "Enterprise Resource Planning (ERP) Implementation Planning and Structure: A Recipe for ERP Success". SIGUCCS'04. Oct. 10-13. 2004.

[31] A. Kern. "Advanced Features for Enterprise-Wide Role-Based Access Control". Proceedings of 18th ACSAC. 2002.

[32] A. K. Harikumar, R. Lee, C. Chiang, and H. Yang. "An Event Driven Architecture for Application Integration using Web Services". IRI-2005 IEEE International Conference on. pp. 542-547. 15-17 Aug. 2005.

[33] M. Themistocleous, Z. Irani, R. M. O'Keefe,and R. Paul. "ERP Problems and Application Integration Issues: An Empirical Survey". Proceedings of the 34th Hawaii International Conference on System Sciences. 2001.

[34] G. Kolaczek. "Specification and Verification of Constraints in Role Based Access Control for Enterprise Security System". Proceedings of the Twelfth IEEE International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises. 2003.

[35] D.C. Merrill, A. MacWillson, G. Loveland. "Requirements for a true Enterprise-Wide Security Infrastructure: The play's the thing". The 17th IEEE Symposium on Reliable Distributed Systems. pp. 403. 1998.

[36] A.K. Harikumar, R. Lee, H. S. Yang, H. Kim, and B. Kang. "A Model for Application Integration using Web Services". Proceedings of the Fourth Annual ACIS International Conference on Computer and Information Science. 2005.

[37] T. Mukhopadhyay, S. Kekre, and S. Kalathur. "Business Value of Information Technology: A Study of Electronic Data Interchange". MIS Quarterly/June 1995.

[38] F. Shafiei, and D. Sundaram. "Multi-Enterprise Collaborative Enterprise Resource Planning and Decision Support Systems". Proceedings of the 37th Hawaii International Conference on System Sciences. 2004.

[39] White Paper. "my SAP ERP Solution Overview". SAP AG. 2006.

[40] A. Scheer, and F. Habermann. "MAKING ERP A SUCCESS *Using business process models to achieve positive results*". Communications of the ACM. Vol.43. No.4. Apr. 2000.

[41] White Paper. "R/3 System: SAP R/3 on OS/390". SAP AG. 1999.

[42] Y. Baghdadi. "A Web Services-Based Business Interactions Manager to Support Electronic Commerce Applications". ICEC'05, 15-17 Aug., 2005.

[43] White Paper. "Business Process Management with SAP NetWeaver". SAP AG. 2004.

[44] White Paper. "A Business View of mySAP CRM". SAP AG. 2001.

[45] B. Kezmah, and I. Rozman. "Web Services in ERP Solutions: A Managerial Perspective". MIS 2002, LNCS 2641, pp. 177–179, 2003.

[46] R. Chandramouli. "Enterprise Access Policy Enforcement for Applications through Hybrid Models and XSLT Technologies". ICEC'04, Sixth International Conference on Electronic Commerce. 2004.

[47] W. P. Melling. "Enterprise Information Architectures - They're Finally Changing". SiGMOD'94. May. 1994.

[48] C. Bussler. "The Role of B2B Engines in B2B Integration Architectures". SIGMOD Record. Vol.31. No.1. Mar. 2002.

[49] H. Lin, P. Hsu, J. Leu, and W. Tsai. "An Analysis of ERP Systems Based on N-tier Architecture". 26th Int. Conf. information Technology Inteffaces /TI 2004. Jun. 7-10. 2004.

[50] A. Dabkowski, and A. M. Jankowska. "Comprehensive Framework for Mobile ERP System". Proceedings of the 14th International Workshop on Database and Expert Systems Applications. 2003.

[51] M. L. Markus, C. Tanis, and P. C. van Fenema. "Multisite ERP Implementations". Communications of the ACM. Vol.43. No.4. Apr. 2000.

[52] B. Dietrich. "Resource Planning for Business Services". Communications of the ACM. Vol. 49. No.7. Jul. 2006.

[53] Y. Yao, and H. He. "Data Warehousing and the Internet's Impact on ERP". IT Pro. Mar/Apr. 2000.

[54] L. Frank. "Electronic Commerce Using Distributed ERP-Systems with Approximated ACID Properties". Proceedings of the 34th Hawaii International Conference on System Sciences. 2001.

[55] C. P. Holland, and B. Light. 'Global Enterprise Resource Planning Implementation". Proceedings of the 32nd Hawaii International Conference on System Sciences. 1999.

[56] G. A. S. Torrellas. "A Framework for Multi-Agent System Engineering using Ontology Domain Modelling for Security Architecture Risk Assessment in E-Commerce Security Services". Proceedings of the Third IEEE International Symposium on Network Computing and Applications. 2004.

[57] Z. Pozgaj. "Information collected in the biometric identification process should be used in Enterprise Resource Planning". 25th Int. Conf. Information Technology Interfaces IT1 2003, Jun. 16-19. 2003.

[58] A. Wang, and X. Tu. "Intelligent Autonomous Decentralized Enterprise Resource Planning". Autonomous Decentralized Systems, 2005.

[59] B. Ye, Z. Ma, C. Wang, and X. Tu. "Research on the Architecture of Distributed Intelligent ERP System". Networking, Sensing and Control, 2005.

[60] L. Hayman. "ERP in the Internet Economy". Information Systems Frontiers 2:2. pp.137-139. 2000.

[61] Z. SZITAS. "Technical requirements in Enterprise Resource Planning systems". 2th Int'l Spring Seminar on Electronics Technology.2004.

[62] W. Li, and L. Peng. "Upgrade ERP from C/S to B/S Based on Web Service". Services Systems and Services Management. 2005.

[63] S. Dumbrava, and I. M. Valova. "The Design of an Enterprise Resource Planning Software Application for Manufacturing Control". Computer as a Tool, 2005.

[64] C. Rolland, and N. Prakash. "Bridging the Gap Between Organisational Needs and ERP Functionality". Requirements Eng. 5:180-193. 2000

[65] V. Leopoulos, K. Kirytopoulos, and D. Voulgaridou. "ERP systems as a component of the electronic supply chain: Classification of implementation risks". CIMCA-IAWTIC. 2005.

[66] H. Klaus, M. Rosemann, and G. G. Gable. "What is ERP?". Information Systems Frontiers 2:2. pp.141-162. 2000.

[67] D. Kehagias, K. C. Chatzidimitriou, A. L. Symeonidis, and P. A. Mitkas. "Information Agents Cooperating with Heterogenous Data Sources for CustomerOrder Management". ACM Symposium on Applied Computing. 2004.

[68] A. Gupta. "Enterprise Resource Planning: the Emerging Organizational Value Systems". Industrial Management & Data Systems. 100/3. pp. 114-118. 2000.

[69] D. C. Yen, D. C. Chou, and J. Chang. "A Synergic Analysis for Web-based Enterprise Resource Planning Systems". Computer Standards & Interfaces. 24. pp.337-346. 2002.

[70] Kapil Apshankar. "Web Services Architecture". http://www.webservicesarchitect.com/content/articles/apshankar01.asp.